US006477645B1

(12) **United States Patent**
Drews

(10) **Patent No.: US 6,477,645 B1**
(45) **Date of Patent: Nov. 5, 2002**

(54) **AUTHORITY AND INTEGRITY CHECK IN SYSTEMS LACKING A PUBLIC KEY**

(75) Inventor: **Paul C. Drews**, Gaston, OR (US)

(73) Assignee: **Intel Corporation**, Santa Clara, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/243,663**

(22) Filed: **Feb. 3, 1999**

(51) **Int. Cl.**[7] **G06F 1/24**

(52) **U.S. Cl.** **713/168**; 713/170; 713/176; 713/180; 713/182

(58) **Field of Search** 713/168, 170, 713/176, 180, 182

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,264,782 A		4/1981	Konheim	178/22
5,005,200 A		4/1991	Fischer	380/30
5,420,927 A		5/1995	Micali	380/23
5,465,299 A		11/1995	Matsumoto et al.	380/23
5,953,420 A	*	9/1999	Matyas et al.	380/285
6,190,257 B1	*	2/2001	Takeda et al.	463/29
6,292,896 B1	*	9/2001	Guski et al.	713/169

* cited by examiner

Primary Examiner—Thomas R. Peeso
(74) *Attorney, Agent, or Firm*—Schwegman, Lundberg, Woessner & Kluth, P.A.

(57) **ABSTRACT**

A system for checking the integrity and authority of information includes a user platform, a communication channel, and a remote platform. The remote platform transmits the information to the user platform via the communication channel. The user platform, which lacks a public key for the information, verifies the authority and integrity of the information by comparing a transformation value of the information generated on the platform to a transformation value supplied by a user. The platform is also capable of authenticating the information by displaying the transformation value generated from the information and requesting that the user match the transformation value generated from the information with a transformation value known to the user.

36 Claims, 3 Drawing Sheets